



G-Cloud 15 (RM1557.15)

CLEO Systems 24 LTD

**CLEO Integrated Urgent Care (IUC)
Service Definition**

January 2026

Table of contents

1 Introduction	4
1.1 Document structure.....	4
1.2 How to use this document	4
2 Service description	5
2.1 About our service	5
2.2 Delivery framework.....	5
2.3 Service features / benefits	6
2.4 Service scope	7
2.4.1 Add-ons and extensions	7
2.4.2 Cloud deployment model	8
2.4.3 Service constraints	8
2.4.4 System requirements.....	9
2.5 User support.....	9
2.5.1 Support details.....	9
2.5.2 Accessibility and usability	10
2.6 How users work with our service.....	11
2.6.1 Browsers	11
2.6.2 Desktop application	11
2.6.3 Mobile.....	11
2.6.4 Service interface	11
2.6.5 API	11
2.6.6 Accessibility and usability	12
2.6.7 Customisation	12
2.6.8 Service levels and availability.....	12
3 G-Cloud alignment information	14
3.1 Section introduction	14
3.2 Onboarding and offboarding processes.....	14
3.2.1 Onboarding	14
3.2.2 Offboarding.....	14
3.3 Data	15
3.3.1 Data importing and exporting	15
3.3.2 Analytics	15
3.3.3 Independence of resource	16
3.3.4 Public sector networks	16
3.3.5 Data-in-transit protection	16
3.3.6 Asset protection	16
3.4 Availability and resilience	17
3.4.1 Guaranteed availability	17

3.5 Governance	17
3.6 Security	18
3.6.1 Operational security	18
3.6.2 Staff security	19
3.6.3 Secure development	19
3.6.4 Identity and authentication	19
3.7 Auditing	19
3.7.1 Performance monitoring and metrics	19
3.7.2 Compliance and quality management	20
3.8 Backup, restore & disaster recovery	20
3.9 Training	21
3.10 Service pricing	22
3.11 Invoicing process	22
3.12 Termination terms	22
4 Security and data governance	23
4.1 Data protection and encryption	23
4.2 Data at rest, storage locations and physical security	23
4.3 Data sanitisation and disposal	23
4.4 Security testing and assurance	23
4.5 Incident and protective monitoring management	23
4.6 Configuration and change management	24
4.7 Information security management and certifications	24
4.8 Secure development and cryptography	24
4.9 Identity and access management	24
5 Supplier information	25
5.1 About us	25
5.2 Relevant experience and testimonials	25
5.3 How to buy	27

1 Introduction

1.1 Document structure

This Service Definition outlines how CLEO Integrated Urgent Care (IUC) will be delivered under the G-Cloud 15 framework. We have structured the document to give public-sector customers clear, accessible information about the service. This includes its functionality, delivery model, technical requirements, security standards and commercial terms. To support customers at different stages of the procurement lifecycle, we have organised this document into 5 main sections:

- **Section 1 – Introduction:** Provides an overview of the purpose of this document, how it is organised and how it should be used by customers evaluating CLEO IUC
- **Section 2 – Service description:** Describes what CLEO IUC is, the problems it solves, the service features and benefits, technical requirements, service levels and how end-users interact with the system
- **Section 3 – G-Cloud alignment information:** Demonstrates how CLEO IUC meets the specific requirements of the G-Cloud 15 framework, including onboarding/offboarding processes, data controls, service availability, governance, security and auditability
- **Section 4 – Security and data governance:** Details how CLEO IUC protects patient data, maintains compliance with NHS and UK Government standards and embeds security throughout its technical and operational environments
- **Section 5 – Supplier information:** Provides background on CLEO Systems, our experience, customer base and how to purchase CLEO IUC through the G-Cloud Digital Marketplace

We have structured each section to allow customers to quickly locate the information most relevant to their stage in the procurement process.

1.2 How to use this document

This Service Definition has been designed to guide customers through the G-Cloud procurement process and provide clear, structured information about CLEO IUC. It can be used to:

- Assess service suitability with Section 2 summarising what CLEO IUC does, the settings it supports and the problems it solves, helping alignment with local healthcare needs
- Complete technical and security due diligence as Sections 3 and 4 outline hosting, data protection, onboarding, availability, resilience, compliance and governance
- Plan implementation and operational readiness through Section 3's detailing of onboarding activities, prerequisites, roles and training expectations
- Support commercial and contractual review with Section 3.10-3.12, providing pricing models, invoicing approach and termination terms
- Verify supplier capability as we have outlined our organisation background, accreditations and relevant NHS experience in Section 5

2 Service description

2.1 About our service

CLEO Systems provides secure, clinically aligned urgent care solutions designed to support NHS organisations across IUC settings. This includes community-based services such as:

- NHS 111
- Clinical Assessment Services
- Urgent Treatment Centres
- Same Day Emergency Care

Founded in 2019 in Ashford, Kent, we operate as a UK-based subsidiary of the IC24 Group, demonstrating our healthcare expertise and long-standing commitment to public-sector delivery.

Ensuring patients receive timely and appropriate care, our CLEO IUC service enables patients to navigate seamlessly through their entire urgent care journey, from first contact to discharge. By streamlining clinical workflows and enhancing interoperability, CLEO IUC helps organisations address key challenges such as:

- Reducing delays and improving patient flow
- Enhancing clinical safety and data security
- Supporting national priorities for integrated urgent and emergency care
- Improving sustainability through reduced paper usage and efficient digital processes

These outcomes align with the NHS Long Term Plan and wider transformation programmes, including digital-first urgent care and improved access to remote consultations.

Verifying that our service remains intuitive, clinically safe and grounded in real operational practice, we shape our approach through our in-house clinicians. Providing robust data protection and system integrity assurance, we hold **Cyber Essentials Plus** certification and comply with the NHS Digital Data Security and Protection Toolkit (NHS DSPT).

Offering a practical route for organisations seeking a low-disruption, high-impact urgent care solution, CLEO IUC combines flexibility, interoperability and proven safety. Under the G-Cloud 15 Framework, we provide a trusted, scalable service that helps clinical teams work more efficiently, reduce operational risk and deliver better experiences for patients.

2.2 Delivery framework

Designed to provide a safe, predictable and efficient transition to live service, we deliver CLEO IUC through a structured, clinically informed delivery framework. Ensuring consistency across all implementations, our approach supports buyers from initial mobilisation through configuration, training, testing, go-live and ongoing optimisation.

Our delivery lifecycle combines clinical engagement, technical readiness and robust governance. We begin by confirming service scope, interoperability requirements and user roles, before configuring the environment, providing targeted training and supporting end-to-end testing. Once live, we deliver a short period of enhanced support before transferring the service to Business-As-Usual (BAU) operation, supported by our Service Desk, Account Management Team and continuous improvement processes.

We designed our delivery framework this way to minimise disruption, accelerate adoption and ensure clinical safety at every stage. We underpin each phase with defined responsibilities, transparent communication and

alignment with NHS digital-safety standards. This enables our customers to adopt CLEO IUC quickly, reduce operational risk and achieve measurable benefits from the outset.

Our visual delivery framework and lifecycle diagram:

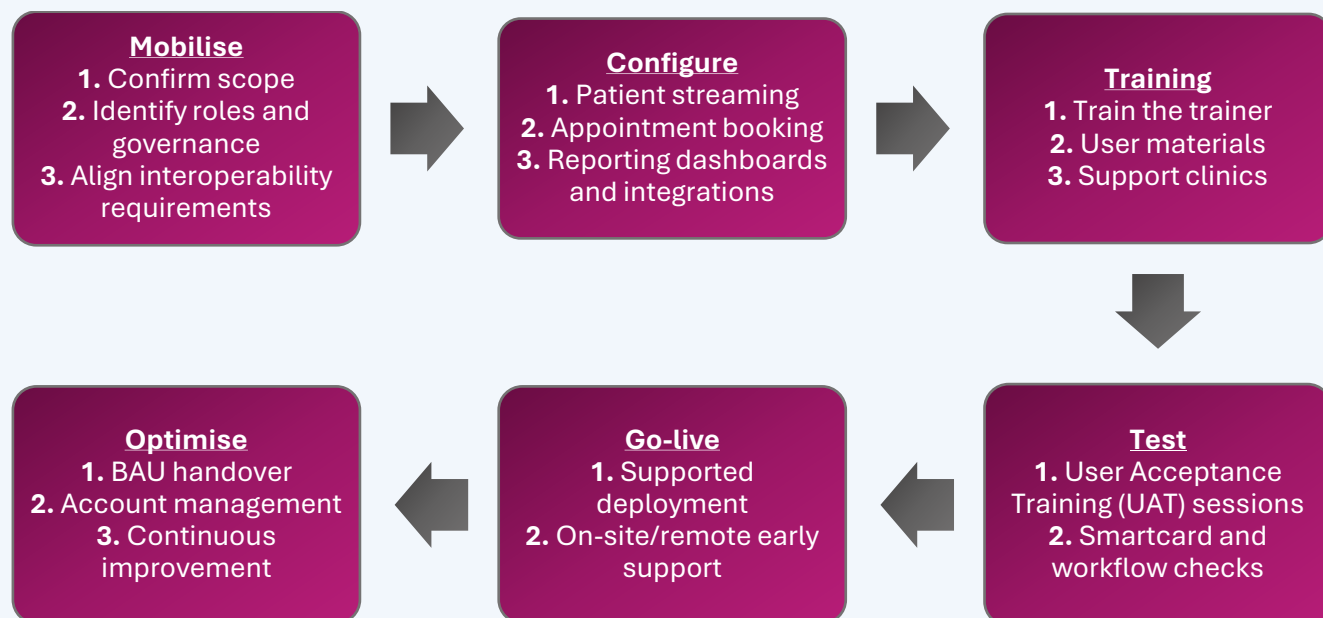


Figure 2.2.1: Our visual delivery lifecycle diagram

2.3 Service features / benefits

To streamline urgent care workflows, improve patient safety and enhance operational efficiency, CLEO IUC provides a comprehensive suite of features designed. Key features include:

- **Spine-connected electronic prescribing:** CLEO IUC connects securely to the NHS Spine to enable electronic prescription transfers to any community pharmacy
- **Patient streaming and redirection:** Direct patients to the most appropriate care setting quickly and safely
- **Digital Appointment Booking (DAB):** Manage the full patient pathway from first contact to discharge or referral
- **Electronic prescribing:** Integrated prescribing workflows for urgent care settings, reducing reliance on paper FP10s
- **GP Connect and Care Connect Integration:** Real-time access to patient records and seamless data sharing across care settings
- **Virtual consultations:** Secure video and audio consultations to support remote care delivery
- **Speech and text analysis:** Advanced analytics to improve clinical decision-making and service quality
- **Dashboard and data-rich reporting:** Real-time insights for performance monitoring and operational planning
- **Booking and Referral Standard (BaRS) compliance:** Ensures adherence to national standards for urgent and emergency care
- **Emergency Care Data Set (ECDS) compliance:** Supports accurate and timely reporting for national requirements
- **Interoperability with NHS services:** Connects with MIG, PDS, SCR, CPIS, ITK, DoS and other third-party urgent care solutions

By providing these features, CLEO IUC provides a suite of key benefits for our customers, including:



Enhanced clinical safety, through structured workflows and real-time data to reduce the risk of errors and improve decision-making



Improved patient experience through flexibility as we offer patients timely appointments, virtual consultations and seamless care pathways



Operational efficiency gains through the optimisation of staff allocation and increased consultation capacity



Faster patient flow with reduced waiting times and improve throughput across urgent care settings



Data-driven insights with access rich reporting and dashboards to support continuous improvement and strategic planning



Sustainability and cost savings through reduced paper usage, postage and administrative overheads to support greener healthcare



Interoperability and compliance through CLEO IUC's seamless integration with NHS services and adherence to BaRS and ECDS standards

2.4 Service scope

CLEO IUC is a Software-as-a-Software (SaaS) patient management solution delivered as a private-cloud service, designed to support NHS urgent and emergency care settings. This includes NHS 111, Clinical Assessment Services, Urgent Treatment Centres, Same Day Emergency Care and community-based services. To optimise implementation and ensure compliance, we define the scope of CLEO IUC through 4 elements:

- Service characteristics
- Add-ons and extensions
- Cloud deployment model
- Operational constraints and system requirements

This structure helps customers understand how CLEO IUC fits into their environment and which conditions support a smooth adoption.

2.4.1 Add-ons and extensions

CLEO IUC is not an add-on or extension to another software service. It is a standalone solution that can operate independently while integrating seamlessly with NHS services such as GP Connect, PDS, SCR and other urgent care systems.

2.4.2 Cloud deployment model

Providing controlled data residency, strong security and predictable performance in compliance with NHS DSPT, we deliver CLEO IUC as a private-cloud SaaS service. To deliver this, we:

- Ensure data remains fully sovereign by hosting all components within UK-based private cloud infrastructure
- Protect performance and support safe urgent care workflows through use of a single-tenant-per-customer model
- Confirm performance during peak activity by designing all environments for scalability
- Enable consistent patching, maintenance and availability by managing the environment centrally

2.4.3 Service constraints

1. Technical and environmental constraints

- Users must authenticate using **NHS Smartcards**, supported by **NHS Digital Identity Agent V2 or above**
- End-user devices must meet the minimum CLEO IUC system specifications
- A **reliable Health and Social Care Network (HSCN) connection** is required at all locations using the service
- Smartcard roles and activities must be correctly configured on all user cards before use
- Local devices must have all CLEO IUC prerequisites installed, including **Java Runtime Environment v8 (32-bit), Microsoft Visual C++ Redistributable 2019 and the Identity Agent registry setting `SessionLockPersistence_Enabled = false`**
- Customers must ensure all devices pass local Acceptance Testing prior to go-live

2. External dependencies

- **NHS Spine** for Smartcard authentication and demographic lookups through the Personal Demographics Service (PDS)
- **PDS** for patient identity matching
- **Summary Care Record (SCR) and GP Connect** integrations for clinical information retrieval
- **Directory of Services (DoS), MIG, ITK-based flows**, as well as **third-party primary care, 999 and digital front door systems** where required by the local configuration
- **HSCN routing and firewalls** configured by the customer

3. Maintenance windows

- We schedule planned maintenance **outside core support hours (08:00-18:00, Mon-Fri)**
- We notify customers of maintenance in advance through the Service Desk or Customer Portal
- Critical updates may require accelerated deployment to maintain clinical safety
- Maintenance releases must be installed promptly to ensure system integrity and all environments must remain aligned with the supported release version
- Release and technology-refresh cycles follow CLEO's structured 8-stage release process:

1. Planning	2. Development	3. Testing	4. Staging
5. Deployment	6. Monitoring	7. Documentation	8. Post-release

4. Geographic and performance considerations

- CLEO IUC is designed for UK-based use only, as it depends on HSCN and NHS national services
- Performance may reduce outside the UK due to the absence of HSCN routing

- System performance is contingent on local infrastructure quality, including workstation spec, local network stability and adherence to CLEO's supported environment standards

2.4.4 System requirements

Requirement	Details
Operating system	Windows 10 or later (1709+)
Processor	Dual-core 2GHz or faster
Memory	Minimum 512MB dedicated to CLEO (typical usage ~240MB)
Install space	100MB per user for installation
Display	Optimal 1920x1080 resolution. Lower resolutions supported but may require scrolling
Frameworks and runtimes	• .NET Framework 4.8 • Java Runtime Environment v8 32-bit (required for NHS Identity Agent) • Microsoft Visual C++ Redistributable for Visual Studio 2019
Smartcard and identity middleware	• NHS Digital Identity Agent V2.4.10.0+ • SessionLockPersistence_Enabled = false under: HKEY_LOCAL_MACHINE\Software\WOW6432Node\HSCIC\Identity Agent • Gemalto Middleware (Identity Agent requirement)
Graphics requirement	Intel Graphics drivers must be up to date (e.g. v30.0.100.9955) due to known compatibility issues with WPF/Chromium-based apps
Connectivity	• Full access to NHS HSCN • Appropriate firewall configuration for CLEO IUC, PDS, SCR and connected services
Smartcard access	Users must have valid Smartcards with the correct roles and activities applied
API integration (optional)	API available (PDF documentation) with test and sandbox environments supported
Compatibility	Windows-only (not compatible with macOS, iOS, Android or Linux)

Figure 2.4.4.1: CLEO IUC system requirements

2.5 User support

To help users resolve issues quickly and maintain safe prescribing, we provide a structured, ITIL-aligned support service. To deliver this, our Service Desk triages requests, allocates skilled specialists and ensures rapid, consistent support across all clinical settings. Strengthening operational continuity, we combine multi-channel access, clear escalation routes and proactive account management.

2.5.1 Support details

How users contact us

User can access support through the following channels:

- **Customer Portal:** For logging incidents, service requests and change requests
- **Email:** For non-urgent queries - support@cleosystems.com
- **Telephone:** For Priority 1 (Critical) incidents, available 24/7

To ensure all support is delivered by trained specialists, we do not offer web chat or AI-driven chatbots.

Support hours

To maintain continuity in clinical services, we provide the following support hours:

- **Core support hours:** 08:00-18:00, Monday-Friday (UK time)
- **Critical incident support:** 24/7 by telephone for Priority 1 cases

- **Portal access:** Available 24/7 for logging and tracking cases

Response times

- ✓ **PRIORITY 1: 1 hour to respond, 4 hours to resolve**
- ✓ **PRIORITY 2: 2 hours to respond, 16 hours to resolve**
- ✓ **PRIORITY 3: 8 hours to respond, 5 business days to resolve**
- ✓ **PRIORITY 4: 8 hours to respond, 30 business days to resolve**

Demonstrating our rapid response times, we maintain **99.9% service availability** and use all reasonable endeavours to **respond to and resolve 100% of support requests within their allocated time**, providing updates accordingly.

Accessibility of support channels

To support all users, our Customer Portal is actively progressing toward WCAG 2.2 AA compliance, with all features supporting keyboard navigation and screen-reader access.

Named support roles

To strengthen governance and communication, we provide the following customer support roles within our Account Management Team:

- A **Customer Success Manager** who provides strategic engagement, reviews performance and aligns the service to buyer priorities
- A **Support Manager** who oversees operational responses and ensures timely incident progression
- A **Project Manager** who supports onboarding and all major service changes

Third-party access

To support shared-service models and multi-agency working, where authorised by the customer, third-party contractors can access the Customer Portal and raise cases.

Escalation routes

The below escalation model ensures rapid action when incidents impact clinical service:



Figure 2.5.1.1: Our escalation routes

This approach protects clinical operations and ensures transparent communication at every stage.

2.5.2 Accessibility and usability

We design our support and user-facing services to be accessible to a wide range of clinical and administrative users, including those who rely on assistive technologies. To promote equitable access, we ensure the following:

- All support services are designed in alignment with WCAG 2.2 AA principles
- Ensure the Customer Portal is accessible through keyboard navigation and screen readers
- Provide documentation in PDF format designed for accessibility, with alternative formats available upon request
- Review accessibility feedback through our robust continuous improvement process

To maintain accessibility across new releases, we undergo comprehensive testing and assurance procedures. Prior to deployment, we assess major updates for accessibility. We review portal usability with real users and integrate emerging accessibility needs into development. Supporting inclusive digital access, we ensure that TOPdesk, our ITSM platform provider, actively develops toward full WCAG 2.2 AA compliance.

2.6 How users work with our service

2.6.1 Browsers

CLEO IUC does not operate in a web browser. Providing consistent performance, our service uses a Windows desktop application.

2.6.2 Desktop application

CLEO IUC uses a dedicated Windows desktop application to support safe, efficient and fully integrated urgent-care operations. We supply the CLEO IUC MSI for the customer to install on approved devices through the customer's endpoint-management tools, whilst we undertake the implementation of the backend services and databases. Customers deploy the CLEO IUC MSI to approved devices through their endpoint-management tools. Key characteristics of our desktop application include:

- Runs on Windows 10 or later (1709+)
- Uses NHS Smartcard authentication through Identity Agent V2.4.10.0+
- Provides real-time connections to PDS, SCR, GP Connect, DoS, MIG and other NHS interoperability services
- Integrates clinical triage, patient streaming, appointment booking and virtual consultation workflows
- Central deployment to verify consistent configuration and reduce local IT overhead

2.6.3 Mobile

CLEO IUC is not designed for use on mobile devices.

2.6.4 Service interface

To support efficient clinical use, we design the CLEO IUC interface around clarity, safety and ease of navigation. Our interface features include:

- Simple, task-focused workflows for triage, streaming and clinical decision-making
- Structured patient-search screens using PDS matching criteria
- Integrated appointment booking, virtual consultation and document sharing views
- Queue oversight tools that allow clinicians to manage caseloads safely
- Real-time dashboards and reporting components to support operational visibility
- Consistent User Interface (UI) design across modules to minimise training time and support rapid adoption

2.6.5 API

CLEO IUC provides incoming and outgoing APIs to support integration with approved NHS services and local services. Buyers have access to a dedicated test and sandbox environment, and full documentation is supplied in PDF format. Through the CLEO IUC API framework, organisations can:

- Integrate with clinical systems using NHS-recognised standards
- Exchange data with GP Connect, Care Connect, MIG and ITK-based services
- Retrieve operational and performance data through secure reporting feeds

- Support interoperability with video consultation, digital front-door and third-party urgent care solutions
- Connect securely to local Business Intelligence (BI) and analytics tools via controlled exports

2.6.6 Accessibility and usability

We designed CLEO IUC's UIs and support services with accessibility at the forefront of its development. Our Customer Portal provider (TOPdesk) is actively working toward WCAG 2.2 AA compliance, incorporating accessibility into its design system and testing approach. Current platform capabilities include:

- Support for keyboard navigation and screen-reader tools
- Accessible PDF documentation, with alternative formats available upon request
- Ongoing improvements based on user feedback and accessibility reviews

We monitor system updates from TOPdesk and incorporate accessibility enhancements into its continuous improvement processes.

2.6.7 Customisation

CLEO IUC includes a range of configurable settings that allow organisations to tailor the service while maintaining clinical safety and operational consistency. User administrators can configure local settings, while CLEO Systems manages advanced and system-wide configurations. Customisable elements include:

- User setup and role-based access permissions
- Organisational settings such as locations, services and care pathways
- Integration enablement, such as with GP Connect, digital appointment booking and virtual consultations
- Local reporting requirements through Secure File Transfer Protocol (SFTP) data feeds
- Queue, workflow and triage configuration within agreed safety parameters

This balanced model ensures flexibility while preserving system integrity across urgent care environments.

2.6.8 Service levels and availability

Ensuring consistent performance and timely support under the G-Cloud 15 framework, CLEO IUC operated under the following Service Level Agreements (SLAs). To continuously monitor system behaviour, we review performance metrics with customers during quarterly account management meetings.

Metric	Target	How we measure it
Service availability	99.9%	Automated uptime monitoring/reporting
Priority 1 response time	1 hour	Recorded in Service Management Tool, allocated a Priority with the customer receiving case reference number
Priority 1 resolution time	4 hours	Request completion log
Priority 2 response time	2 hours	Recorded in Service Management Tool, allocated a Priority with the customer receiving case reference number
Priority 2 resolution time	16 hours	Request completion log
Priority 3 response time	8 hours	Recorded in Service Management Tool, allocated a Priority with the customer receiving case reference number
Priority 3 resolution time	5 business days	Request completion log

Priority 4 response time	8 hours	Recorded in Service Management Tool, allocated a Priority with the customer receiving case reference number
Priority 4 resolution time	30 business days	Request completion log

Figure 2.6.8.1: Our service levels and availability

To maintain these SLAs, we monitor CLEO IUC **24/7** and immediately escalate Priority 1 incidents to our Senior Management Team when required. If an outage occurs, we notify nominated contacts by email and publish updates through a service-status webpage. Full incident reports follow within the agreed contract timeframes. We provide secure daily Single File Transfer Protocol (SFTP) data feeds and scheduled reports on prescribing and system usage, with additional metrics available on request.

Support hours

To maintain continuity in clinical services, we provide the following support hours:

- **Core support hours:** 08:00-18:00, Monday-Friday (UK time)
- **Critical incident support:** 24/7 by telephone for Priority 1 cases
- **Portal access:** Available 24/7 for logging and tracking cases

3 G-Cloud alignment information

3.1 Section introduction

To support safe and efficient prescribing, we deliver CLEO IUC through a structured, collaborative delivery model. To achieve this, we combine defined project controls with flexible engagement, allowing us to meet the needs of diverse clinical environments. Our approach ensures clarity, accountability and strong governance from contract signature to service closure. This section explains how we work with buyer teams during onboarding, configuration, go-live, live-service operation and secure offboarding.

3.2 Onboarding and offboarding processes

For safe, controlled transitions in and out of service, we design onboarding and offboarding processes to give buyers confidence and maintain compliance. Our onboarding approach has been developed to provide a structured and predictable process which aligns with NHS governance requirements. For offboarding, our approach provides full data portability, transparent activity, user control and zero vendor lock-in.

3.2.1 Onboarding

Reducing implementation risk and enabling rapid adoption, our onboarding process establishes the governance, responsibilities and technical readiness required to deploy CLEO IUC safely. Leading users through this process will be a dedicated Project Manager, who will guide clinical, technical and operational teams through each implementation stage.

1. **Kick-off and scoping:** To establish shared expectations, we meet our customer's project and governance teams to confirm scope, timelines and success criteria
2. **Quote:** To formalise delivery, we produce a detailed quote outlining deliverables, dependencies, risks, roles, responsibilities and commercial terms
3. **Access and environment setup:** To enable authentication, our customer prepares Smartcards and assigns the required Roles and Activities. Maintaining security, we ensure the customer has HSCN connectivity and deploys the CLEO IUC MSI package to approved devices. We then validate that prerequisites such as NHS Identity Agent and associated middleware are installed
4. **Resource allocation and scheduling:** Ensuring clear accountability, we assign delivery roles, agree schedules and document milestones within a structured/shared project plan
5. **Discovery and requirements confirmation:** Confirming readiness, we conduct technical and clinical workshops to validate local requirements, align operational processes, including formulary configuration and reporting needs. Furthering this, we facilitate As-Is and To-Be mapping with NHS England where required
6. **Training and User Acceptance Training (UAT) preparation:** Preparing a safe rollout, we deliver Train the Trainer sessions and supply user guides and videos in PDF and MP4 formats respectively. Assuring readiness, users conduct UAT in either a dedicated test environment or the live environment with test patients. After UAT, we require users to complete the DCB0129 to legally certify that the new IT system is safe for live patient care

We conclude onboarding once the user approves UAT, completes governance checks, including DCB0129, and confirm readiness for deployment and go-live. To ensure safe transition, CLEO Systems provides onsite or remote support during go-live, followed by 2 weeks of early-implementation support before transferring to BAU.

3.2.2 Offboarding

To support a secure, transparent exit, we deliver a controlled offboarding process. This returns all buyer data, removes access and allows services to end without disruption. Providing expert oversight of this process will be our Project Management Team.

1. **Project closure review:** Confirming completion, we meet with the user to review deliverables, capture lessons learned, assess performance metrics and gather feedback
2. **Documentation and handover:** Supporting continuity, we provide final configuration outputs, test records, training assets and any required technical documentation
3. **Knowledge transfer:** For user self-sufficiency, we deliver targeted handover sessions with their teams to explain operational workflows, outstanding actions and confirm their competency
4. **Access revocation and data return:** Protecting confidentiality, in line with our Cyber Essentials Plus certification and NHS DSPT compliance, we remove all CLEO Systems access and return data through secure SFTP in agreed CSV formats. Supporting governance, we delete retained data within 3 months and issue a certificate of deletion
5. **Post-engagement support:** Maintaining service continuity, we offer advisory or optimisation through additional quotes where requested

3.3 Data

3.3.1 Data importing and exporting

To ensure full data portability and avoid vendor lock-in, CLEO IUC supports open, non-proprietary data formats for importing and exporting information.

- **Data importing:** CLEO IUC does not require routine data import for clinical workflows. Where project-specific imports are required (for example, configuration data or location/service mappings), these are processed through agreed implementation steps using structured, open formats
- **Data exporting during the contract:** To support local reporting and analytics, we provide secure daily transfers of operational and usage data through SFTP. These structured outputs enable onward processing and may cover:
 - Triage and streaming quality
 - Queue and caseload metrics
 - Appointment booking activity
 - Clinical usage statistics
 - Performance and operational audit fields
- **Data exporting at any time:** Maintaining transparency, customers may request exports of their data at any time. We will supply these in CSV format (or any other agreed open formats), structured to align with local reporting models and data warehouse needs
- **End-of-contract data extraction:** Supporting secure exits, we provide a full and final SFTP data package export in an agreed format such as CSV. Ensuring compliance with our Cyber Essentials Plus certification and the NHS DSPT, we delete supplier-side data **within 3 months** of providing the export and issue a certificate of deletion

3.3.2 Analytics

To help users understand demand, track performance and improve urgent care delivery, CLEO IUC provides rich operational usage metrics. Supporting oversight, we provide metrics covering:

- Triage and clinical assessment volumes
- Queue and caseload management activity
- Appointment booking utilisation
- Operational throughput and workflow patterns
- System usage statistics
- Audit and compliance events
- Speech and text analytics outputs (where enabled)

To integrate easily with local BI platforms, CLEO IUC supports multiple reporting mechanisms:

- Secure daily SFTP data feeds
- Scheduled reports in agreed formats such as CSV and PDF
- Additional on-request extracts to support bespoke dashboards or analytics

3.3.3 Independence of resource

To ensure consistent performance, we deliver CLEO IUC through a private-cloud environment that isolates user environments and prevents cross-tenant interference. Safeguarding stability, we conduct the following:

- Segregate tenant data and infrastructure
- Use load-balanced and resilient hosting environments
- Monitor performance and capacity proactively
- Scale compute resources in line with demand

Through this approach, we maintain service stability during peak periods of urgent care activity.

3.3.4 Public sector networks

CLEO IUC connects securely to the HSCN to support Smartcard authentication and national interoperability. Enabling connectivity, users ensure HSCN access at prescribing locations. Protecting safety, all traffic follows NHS governance requirements. Through this, we provide compliant access to NHS Digital services, including:

- PDS
- GP Connect and Care Connect services
- SCR
- DoS
- MIG
- Video consultation and other integrated urgent care systems

3.3.5 Data-in-transit protection

To protect all data exchanges, CLEO IUC encrypts all data in transit using strong TLS 1.2 or above encryption and secure HTTPS protocols. Preventing internal interception, we secure service-to-service communication using:

- Enforced TLS encryption
- Network segmentation
- Controlled Application Programming Interface (API) gateways
- Secure remote connectivity in line with customer security controls

3.3.6 Asset protection

To protect assets and data, we host all data within UK-based private cloud infrastructure and back it up to separate, segregated cloud environments daily, managed by Arcserve. For data at rest, we apply physical and logical access controls aligned with the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) v3.0, encryption and isolate tenant environments. To sanitise data, we erase user data by explicitly overwriting storage before reallocation, ensuring it cannot be recovered. To sustainably dispose of equipment, we maintain developed CSA CCM v4.0-aligned hardware disposal procedures.

3.4 Availability and resilience

3.4.1 Guaranteed availability

To deliver a consistently reliable service, CLEO IUC maintains 99.9% service availability, supported by controlled private-cloud hosting, continuous monitoring and robust resilience processes. Assuming responsibility for overseeing CLEO IUC's guaranteed availability sits with our CLEO Service Desk Manager, who will oversee platform health, performance and operational continuity.

To uphold 99.9% service availability, we monitor all environments 24/7, receive automatic alerts for anomalies, service-impacting behaviour and potential degradation through our infrastructure and application monitoring tools. To confirm rapid assessment and remediation, we respond to incidents through defined escalation pathways. To prevent outages, we operate CLEO IUC within UK-based private-cloud infrastructure that uses load-balanced servers, isolated resources and secure replication. Protecting performance, we scale resources proactively and separate customer workloads to avoid cross-tenant impact. To guarantee continuity, we back up all data daily to an immutable vault storage and replicate these backups to a segregated cloud environment by Arcserve. For rapid restoration in the unlikely event of disaster scenarios, we follow annually tested disaster-recovery procedures aligned with NHS DSPT and internal Business Continuity Plan controls.

In the event of a service down incident, we triage all incidents immediately and escalate critical issues to senior engineers using our ITIL-aligned process. To protect users during high-security events, we communicate updates immediately through email alerts and a service-status webpage. For transparency, when an outage occurs, we notify all nominated user contacts to provide clear information on:

- Services affected
- Severity
- Issue description
- Actions taken
- Next status update

In the unlikely event of a major incident, we follow up with a full incident report to users within the agreed contractual timeframe.

Supporting consistent service quality, we analyse incident outcomes and integrate improvements into future releases.

3.5 Governance

We deliver CLEO IUC through a robust governance framework that ensures safe, compliant and high-quality service delivery. To achieve this, we combine accredited management systems, structured oversight and continuous improvement processes aligned with NHS and UK Government standards. Demonstrating the strength of our governance procedures, we operate under the following certifications and standards:

- NHS DSPT compliance
- Aligned with NHS England digital standards
- Cyber Essentials Plus

To maintain control and clear accountability, our governance framework management structure includes:

- Data Protection Officer (DPO) who oversees GDPR compliance and DPIA activities
- Information Governance Officer, who provides assurance and escalation in line with NHS IG requirements

To manage risks, we maintain formal change-control processes, which we review annually through a Change Management Board. Furthering this, we update documented risk registers during service reviews, with regular vulnerability scanning and annual penetration testing conducted by CREST-approved providers.

For continuous improvement, we review performance, security and clinical-safety data through structured processes such as:

- Quarterly service reviews to assess performance trends, SLA adherence and customer feedback
- Quarterly internal audits to verify compliance with DSPT, Cyber Essentials Plus and internal security controls
- Annual external audits to validate DSPT and penetration-testing outcomes
- Root-cause analysis following significant incidents to prevent recurrence and strengthen resilience
- Release management reviews ensure new features maintain clinical safety and operational stability

We use the findings from these activities to update our policies, including staff training, refine processes and guide enhancements for CLEO IUC.

3.6 Security

We embed security throughout CLEO IUC to protect patient data, maintain system integrity and comply with UK public-sector standards. Demonstrating this, we combine accredited governance frameworks, continuous monitoring and defined assurance activities overseen by our Information Governance team. Confirming that CLEO IUC is operated using audited, nationally recognised security practices, we align controls with Cyber Essentials Plus and the NHS DSPT. Evidencing strong control maturity, **our latest DSPT external audit reported 0 areas for improvement.**

3.6.1 Operational security

We maintain operational security through controlled change, continuous monitoring and structured incident response. For stability, we assess every change using a formal Change Control Form that records risks, security considerations and implementation details. A Change Management Board reviews all changes and approves safe deployment.

Protecting CLEO IUC users, we monitor threats using an enterprise Security Information and Event Management (SIEM) and Security Operations Centre (SOC) platform. We assess emerging risks through weekly security meetings and intelligence feeds, including NHS CareCERT advisories. We patch critical **vulnerabilities within 72 hours** and high-risk issues **within 14 days**, following NHS CareCERT guidance. Threats we monitor include, but are not limited to:

- Failed logins
- Privilege escalation
- Suspicious network activity
- Baseline deviations

Ensuring high-risk incidents are escalated immediately, we conduct automated risk scoring and alert prioritisation to the on-call security team. We handle all incidents under documented triage, containment, eradication and recovery steps. We communicate progress through user-nominated contacts and issue post-incident reports within agreed timeframes. Following major incidents, we conduct root-cause analysis and corrective actions, feeding improvements back into monitoring rules, playbooks and release processes.

To safeguard operations, we integrate operational security within our Business Continuity Plan (BCP) and disaster-recovery procedures. To confirm readiness, our Governance Officer conducts annual BCP reviews, with any lessons learned from exercises and real events incorporated into our operations.

3.6.2 Staff security

Assuring users that systems are authorised correctly, we only grant access to vetted, authorised staff under least-privilege principles. For example, we screen personnel with access to system or patient data to BS7858 standards before granting access.

3.6.3 Secure development

Managing supply chain risk, we develop CLEO IUC using a secure Software Development Life Cycle (SDLC) that includes threat modelling, peer code review, secure coding standards and dependency scanning. Security assurances we provide also include annual penetration testing by CREST-approved providers, continuous vulnerability scanning and remediation tracking. Through these processes, we confirm that we align with the UK Government Software Security Code of Practice.

3.6.4 Identity and authentication

CLEO IUC ensures only authorised clinicians, call handlers and administrators can access functions that affect patient safety. To achieve this, we apply the following restrictions and safeguards:

- NHS Smartcard authentication through Identity Agent V2.4.10.0+, with the required configuration settings applied in line with national policy
- Verification of Smartcard roles and activities, ensuring access only to permitted clinical workflows
- Restricted administrative access, limited to named and authorised users, with privileged actions fully logged and auditable
- Customer Portal access controlled through username and password authentication, with accounts managed by nominated customer administrators
- Session and activity logging throughout the system to support safety, audit and compliance requirements

3.7 Auditing

To ensure transparency, accountability and compliance with NHS and UK public-sector information-governance standards, CLEO IUC embeds comprehensive auditing across all environments. We record all user activity, including authentication attempts, triage actions, queue management and administrative configuration changes, within secure logs. Ensuring full traceability, we also log all supplier actions performed on behalf of customers.

We securely store audit data within UK-based private-cloud infrastructure and protect it through strict access controls. We retain logs in accordance with customer-defined retention requirements, which can be exported in open formats (such as CSV) for clinical-safety reviews, regulatory audits or internal investigations. Customers may request extracts through the CLEO Systems Service Desk or receive scheduled reports as part of business-as-usual operations.

These auditing capabilities support safe prescribing, assist with incident investigation and underpin compliance with **Cyber Essentials Plus** and the **NHS DSPT**. Our most recent DSPT external audit reported **zero areas for improvement**.

3.7.1 Performance monitoring and metrics

To maintain high service quality and identify emerging issues early, our Live Service Monitoring, Technical Response and Account Management teams oversee the performance of CLEO IUC across all environments.

This includes monitoring operational activity patterns, authentication events, system throughput and overall application behaviour.

Customers receive operational and usage metrics through secure daily SFTP data feeds and scheduled reporting. These outputs support integration with local governance, performance reviews and BI systems. To support more specialised analytical needs, additional or bespoke reporting is available on request.

As part of our collaborative service management approach, we review insights from performance monitoring during scheduled account management meetings. Where deviations from expected performance are detected, issues follow our defined escalation routes, confirming timely investigation and resolution. Enabling rapid intervention if degradation is identified, our monitoring systems provide real-time alerts for infrastructure components, authentication services and application-level functions.

3.7.2 Compliance and quality management

Confirming the quality, safety and consistency of our service, we maintain recognised industry standards and compliance frameworks to deliver CLEO IUC. Demonstrating our commitment to secure operations and strong information governance, we hold **Cyber Essentials Plus** and comply with the NHS DSPT.

Our governance specialists, clinical-safety personnel and information-security teams oversee compliance throughout our service's lifecycle. Protecting service stability, we apply structured ITIL-aligned service management processes, including controlled incident handling, formal change management, documented release procedures and routine problem management reviews.

We conduct annual penetration testing through Tigerscheme or CREST-approved providers, alongside continuous vulnerability scanning and internal audits. Findings from these activities inform our security and service improvement actions.

Through our service and configuration management processes, we maintain full traceability of changes, configuration integrity and audit evidence. To support governance, assurance reviews and regulatory requirements, we retain audit and compliance records in line with customer-defined durations. Allowing us to identify enhancements and agree on corrective actions, we review performance metrics, customer feedback and audit findings as part of our continuous improvement cycle.

3.8 Backup, restore & disaster recovery

Protecting service continuity and safeguarding patient-identifiable data, we maintain a comprehensive, multi-layered backup, restore and disaster-recovery framework for CLEO IUC. To do this, we combine secure immutable storage, segregated replication, robust governance controls and validated recovery procedures aligned with NHS DSPT expectations. Overseeing this will be our Information Governance Team.

Backup and replication

To protect data from corruption, accidental deletion or cyber-threats, we back up all CLEO IUC servers and databases daily to a secure, immutable vault, ensuring backups cannot be altered or overwritten. Strengthening resilience further, we replicate all backups to a separate, segregated cloud environment hosted and managed by Arcserve, providing physical and logical separation from the production platform. Our infrastructure team verifies the successful completion of each backup and monitors for anomalies. To protect retention compliance, all backup data is retained within UK-based cloud regions.

Objectives and governance

CLEO IUC maintains a **Recovery Point Objective (RPO) of 24 hours** and a **Recovery Time Objective (RTO) of 1 hour** for CLEO IUC. To meet these objectives, we operate a suite of disaster-recovery, incident-response, data-breach and IG-incident plans that define decision pathways, activation triggers, communication flows

and escalation responsibilities. Maintaining readiness, our BCP outlines the operational processes we follow during disruptive events, including technology failover, communication routes, team coordination, access controls and restoration sequencing. To ensure alignment with NHS expectations, we test and review the Business Continuity Plan annually, using outcomes to refine procedures and strengthen our recovery approach.

Restoration and assurance

To validate recoverability, we perform regular restoration activities, including controlled drills, database roll-forward checks and system validation testing. Minimising disruption, we maintain documented restoration steps, fallback procedures and prioritised recovery tasks that confirm mission-critical CLEO IUC functions are restored in the correct sequence. To strengthen reliability, we compare restoration outcomes against RPO/RTO targets and adjust technical configurations if performance gaps are identified. Following any continuity event or test exercise, we conduct a post-event review with technical, governance and operational leads. To improve resilience further, we integrate findings into updated procedures and adjust failover processes, communication steps and resource assignments.

End-to-end continuity alignment

To maintain oversight, senior leadership receives reports on disaster-recovery outcomes, readiness testing, identified risks and improvement activity. Ensuring transparency, CLEO Systems shares relevant continuity documentation with buyers upon request and assures that restoration pathways and data recovery activities remain effective.

3.9 Training

CLEO IUC training is designed to ensure clinicians and administrators can use the system safely, confidently and in alignment with NHS standards. Our training supports local capability by building and ensuring smooth adoption during onboarding and go-live.

Training approach

To support an efficient rollout, we follow a Train-the-Trainer model, enabling local super users to cascade training across teams at scale. Super-users receive detailed instructions on:

- Core CLEO IUC navigation
- Triage, streaming and clinical workflow processes
- Queue management and caseload oversight
- User administration and role-based accesses
- Digital appointment booking
- GP Connect and Care Connect integrations
- Virtual consultation workflows
- Reporting dashboards and SFTP data-feed outputs

This helps organisations build internal capability and reduce long-term dependency on external support. Ensuring familiarity with key workflows and system navigation, we deliver this training ahead of User Acceptance Training (UAT).



Figure 3.9.1: Our training materials infographic

These materials support formal training sessions and act as long-term reference tools for end users and administrators, with updates following major releases.

Go-live and ongoing support

We align training with the customer's implementation schedule to support readiness for UAT and go-live. Additional sessions or refresher training can be provided upon request, using SFIA rates where required.

3.10 Service pricing

CLEO IUC pricing is bespoke and tailored to the user's needs, covering licenses, implementation, hosting, managed service, training, SMS messaging and connector costs as required. We price additional services using the SFIA rate card.

3.11 Invoicing process

CLEO Systems invoices annually in advance on contract signature, with 30-day payment terms. We accept standard public-sector payment methods and align with government invoicing practices.

3.12 Termination terms

The minimum contract term for CLEO IUC is 12 months. Customers may end the Call-Off by giving 30 days' written notice, with CLEO Systems ceasing service on the agreed date and customers settling outstanding sums by the termination date. We return all data through SFTP in CSV format or other agreed open formats, with supplier-side data deleted within 3 months and a certificate of deletion provided.

4 Security and data governance

4.1 Data protection and encryption

To protect sensitive data, we encrypt all data in transit using TLS 1.2 or above encryption. To enforce strong authentication and access control, we also encrypt internal service and microservice communication and route it through segmented networks with secure API gateways.

4.2 Data at rest, storage locations and physical security

We only store CLEO IUC within UK-based private-cloud infrastructure. We encrypt data using SQL Server TDE Encryption at rest through physical and logical access controls and tenant isolation. We align our data centre security and asset controls with the CSA CCM. To comply with industry-recognised standards, we are currently working towards aligning these processes with the latest CCM v4.0 controls.

4.3 Data sanitisation and disposal

To ensure deleted data cannot be recovered, we sanitise data by explicitly overwriting storage before reallocation. Where equipment reaches end-of-life, we dispose of it in accordance with recognised standards, such as CSA CCM, and provide certificates of destruction on request.

4.4 Security testing and assurance

We provide assurance of the security of our systems through annual penetration testing by CREST-approved or Tigerscheme-qualified providers and continuous vulnerability scanning across environments. For transparency and auditability, we track findings from identification to remediation, with status reported through service governance and account management engagements.

4.5 Incident and protective monitoring management

To protect CLEO IUC from security threats and ensure safe clinical operation, we maintain continuous protective monitoring supported by our enterprise SIEM and SOC. Further to this, we maintain a structured incident response approach aligned with ISO27035, Cyber Essentials Plus and the NHS DSPT.

- ✓ **Protective monitoring:** We operate 24/7 SIEM and SOC monitoring across CLEO IUC infrastructure, which analyses logs from servers, applications, authentication services and network controls. We escalate alerts for unusual or high-risk activity to our security specialists for investigation
- ✓ **Incident response:** We follow a formal incident response process that includes identifying, assessing and containing threats before restoring normal service. Aligning our processes with recognised NHS and UK Government standards, we escalate high-severity incidents immediately to senior security leaders
- ✓ **Preventative controls:** Minimising risk, we conduct annual penetration testing through CREST or Tigerscheme-approved providers, operate continuous vulnerability scanning and apply risk-based patching following NHS CareCERT guidance
- ✓ **Customer communication:** In the unlikely event of a major incident, we notify nominated customer contacts promptly and provide updates through agreed communication channels. We then issue a post-incident report in line with contractual requirements
- ✓ **Continuous improvement:** Our governance teams review lessons learned from incidents and security events, using them to strengthen monitoring rules, access controls and security configurations

4.6 Configuration and change management

For performance stability, we track configuration items throughout their lifecycle in a Configuration Management Database. Before each release, we assess risk by performing security impact reviews for every change. To authorise updates, our Change Management Board approves deployments and rollback plans. Minimising disruption, we issue full incident reports within the contractually agreed timeframe.

4.7 Information security management and certifications

Managing all information security management procedures for CLEO IUC will be our Information Governance Team. Demonstrating our competence, we hold the following certifications:

- Cyber Essentials Plus
- Compliance with the NHS DSPT

To confirm our compliance, we undergo annual external audits to renew our certifications.

4.8 Secure development and cryptography

We follow secure development practices aligned to recognised standards on a self-assessed basis. We develop CLEO IUC using a secure SDLC, incorporating:

- Threat modelling
- Peer code reviews
- Secure coding standards
- Continuous vulnerability scanning
- Structured release management
- Dependency and vulnerability scanning
- Annual penetration testing by Tigerscheme or CREST-approved providers
- Remediation tracking
- Change controls

All communications are protected using strong cryptographic controls, including TLS 1.2+ for data in transit.

4.9 Identity and access management

CLEO IUC enforces strong authentication and access controls to ensure that only authorised clinicians, call handlers and administrators can access patient information and operational workflows. Access controls include:

- NHS Smartcard authentication through Identity Agent V2.4.10.0+
- Verification of Smartcard roles and activities before enabling access to clinical or operational functions
- Restricting administrative access to named and authorised users only
- Full logging of privileged and security-relevant activity
- Username and password access for the Customer Portal, managed by nominated customer administrators

5 Supplier information

5.1 About us

We are CLEO Systems, a UK health-tech provider within the IC24 Group, delivering intuitive digital solutions that simplify urgent care workflows and improve clinical coordination. Founded in 2019 in Ashford, Kent, we operate as part of a social enterprise, reinvesting surplus to strengthen care quality and support sustainable NHS innovation. We are a specialist organisation with in-house clinicians and digital experts who support product development, testing and iterative improvement across multiple NHS environments.

Supporting safe, efficient and clinically informed patient management, we serve key sectors across the NHS, including:

- Secondary care outpatients
- Community services
- Urgent care
- Community pharmacies

Our organisational mission is to empower clinicians, improve patient experience and increase efficiency through intuitive, clinically informed system design. We use these key values to shape how we plan, deliver and support all of our innovative solutions. We maintain recognised governance and security standards, evidenced by our suite of accreditations shown below:

- NHS DSPT compliance
- Aligned with NHS England digital standards
- Cyber Essentials Plus

Through our **6+ years of experience**, we have delivered digital transformation across urgent care and community settings, reducing administrative burden, strengthening clinical visibility and improving patient flow. Our clients include:

- **BrisDoc Healthcare Services**
- **Bexley Health Neighbourhood Care CIC**
- **East Kent UTC Alliance**
- **Greenwich Health**

5.2 Relevant experience and testimonials

In August 2025, BrisDoc Healthcare Services, the NHS provider that delivers integrated urgent care across Bristol, North Somerset and South Gloucestershire, completed a full transition from their previous urgent care system to CLEO IUC. This represented a major digital transformation across all BrisDoc IUC servicing, including NHS 111, out-of-hours, home visiting and clinical navigation functions.

The logo for BrisDoc, with "Bris" in a teal, sans-serif font and "Doc" in a dark grey, sans-serif font.

Project background and objectives

BrisDoc sought to replace its long-standing IUC system to meet growing demand, increasing operational complexity and the need for higher clinical visibility across urgent care pathways. Their previous system limited efficiency, slowed key workflows and constrained digital integration opportunities across partner systems. BrisDoc needed a platform that would:

- Support safer, faster clinical triage

- Offer deeper interoperability with primary care and system partners
- Improve oversight across NHS 111 and CAS queues
- Reduce clinical and operational friction
- Provide a scalable foundation for long-term service innovation

Our solution

BrisDoc selected CLEO IUC for its:

- ✓ **Strong clinical safety credentials**, aligned to NHS England's digital assurance standards
- ✓ **Interoperability**, including access to GP summary records and seamless integration with EMIS, Connecting Care and other ecosystem partners
- ✓ **Intuitive design**, enabling call handlers and clinicians to work more effectively
- ✓ **Powerful reporting tools**, leading to improved decision-making and operational oversight
- ✓ **Capability across multiple urgent care models** (CAS, NHS 111, UTC, home visiting, clinical navigation)

We worked closely with BrisDoc to deliver a rigorous implementation, including extensive UAT, clinical safety governance and structure go-live support. BrisDoc confirmed that the rollout was **“smooth and successful”**, praising our collaborative engagement approach.

Key improvements and outcomes

Streamlined clinical workflows: We delivered significant workflow enhancements across clinical assessment, booking flows, queue navigation, case review and documentation consistency

Enhanced clinical oversight and governance: Through CLEO IUC, BrisDoc identified the major benefits in breach time visibility, queue transparency, clinical navigator review processes and audit trail completeness

Improved interoperability and information availability: CLEO IUC's integration with GP summary records, EMIS and other systems allowed for:

1. Faster, better-informed clinical decisions
2. Improved shared care coordination
3. Reduction in manual data entry

Faster triage and case progression: We provided BrisDoc with multiple time-saving improvements, including:

- Faster booking processes
- Streamlined mental health scripting
- Spine match optimisation
- More efficient weekend workflows
- Faster case routing to oversight queues

Cost and resource efficiency: Through our design and architecture, BrisDoc achieved lower maintenance/development costs, scalability without additional financial burden and improved workforce utilisation.

Testimonial

BrisDoc:

“CLEO IUC not only meets our clinical needs – it also offers a forward-thinking approach that will support our future growth and technological advancements.”

5.3 How to buy

CLEO IUC can be procured directly through the CCS G-Cloud 15 Digital Marketplace. Customers can search for CLEO Systems on the Digital Marketplace and select the required service listing. Once selected, the customer and CLEO Systems will:

1. Agree a SOW detailing scope, deliverables, timescales and pricing
2. Raise a Call-Off Contract under the G-Cloud framework terms
3. Issue a Purchase Order to confirm commencement

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions.

For any enquiries, please contact:

hello@cleosystems.com
03333 200024